UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/088,336	06/13/2002	Tatsuya Inokuchi		2868

530 7590 06/08/2006

LERNER, DAVID, LITTENBERG,
KRUMHOLZ & MENTLIK
600 SOUTH AVENUE WEST
WESTFIELD, NJ 07090

EXAMINER	
KIM, JUNG W	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 06/08/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/088,336	**Applicant(s)** INOKUCHI ET AL.	
	Examiner Jung Kim	**Art Unit** 2132	

-- The MAILING DATE of this communication appears on th cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 April 2006*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-58* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *26-33 and 47-58* is/are allowed.

6)☒ Claim(s) *1-25,34 and 35* is/are rejected.

7)☒ Claim(s) *36-46* is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *11 April 2006* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *4/06*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. This Office action is in response to the amendment filed on April 11, 2006.

2. Claims 1-58 are pending.

Response to Amendment

3. The objection to the Specification is withdrawn, as the amendments overcome the objection.

4. The 112/1st paragraph rejections of claims 35, 36, 49 and 50, and the respective dependent claims are withdrawn, as the arguments are persuasive. The new drawings including figures 9 and 10 are sufficient to overcome the deficiencies in the application.

5. The 112/2nd paragraph rejections to claims 8, 16 and 26 are withdrawn as the amendment overcomes the 112/2nd paragraph rejections.

Response to Arguments

6. After reviewing the amended claims of the instant application and the amended claims of copending application 10,088,337, it has been found that a provisional double patenting rejection is still warranted. Rejections follow.

7. The 112/2nd paragraph rejections to claims 47-58 are withdrawn, as applicant's arguments are persuasive.

8. Applicant's arguments against the 112/2nd paragraph rejections to claims 1-6 have been fully considered but are not persuasive. Applicant argues that the

authentication step indicated by the examiner is neither essential nor critical steps of the claimed invention. In particular, applicant points to portions of the Specification including the Abstract that suggest an invention that omits the authentication steps. Applicant specifies that this step is "not critical or essential to how the invention of claim 1 processes the data" (pg. 34) However, claims 1-6 are not merely claiming a method to process data but rather a method of recording data; applicant's arguments do not address the fact that claims 1-6 are claiming "a method of recording data to a recording medium" as recited in the preamble of the independent claim. Moreover, in all the enabling portions of the specification, authentication is required prior to exchanging an encryption key: this is an essential step to ensure that the exchange occurs only between authenticated parties. (fig. 5) The purpose for authentication is obvious, exchanging a key with an unauthenticated user is a security flaw. This requirement is more definitely asserted in the claims themselves: the authentication step is essential since the method only records the data to the recording medium when the recorder successfully authenticates the terminal unit. (See claim 2: "when the recorder has not successfully authenticated the terminal unit, data recording to the recording medium is ceased) For these reasons, the 112/2nd paragraph rejections to claims 1-6 are maintained.

9. The indicated allowability of claims 1-7 is withdrawn in view of the newly discovered reference(s) to Bjorn. Rejections based on the newly cited reference(s) follow.

10. Finally, applicant's argument against the prior art rejections with respect to amended claims 8-25 and 34-35 are moot in view of the new rejections under Kupka and Bjorn.

Information Disclosure Statement

11. The IDS certified as being submitted on 9/13/2005 and received on 4/11/2006 has been considered. An initialed copy of the IDS is enclosed.

Drawings

12. The drawings were received on 4/11/2006. These drawings are acceptable.

Double Patenting

13. Claims 16 and 34 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 33, 37, 40, 41, 42, 65 and 73 of copending Application No. 10,088,337. Although the conflicting claims are not identical, they are not patentably distinct from each other because the limitations of these claims are substantial defined in the claims of the copending application.

14. As per claim 16:

a. Regarding the limitations: "when a player is going to play back a recording medium containing user identification information, intended to identify a user, and data having been encrypted with the user identification information and stored in the recording medium therewith, judging whether user identification information read from an information holder provided in the player to hold user identification information sent from a terminal unit is coincident with user identification information read from the recording medium; decrypting encrypted data read from the recording medium when the user identification information read from the information holder provided in the player is coincident with the user identification information read from the recording medium,"

b. These features are recited in copending application no. 10,088,337, claim 33, "comparing recording medium user identification data read from a recording medium upon which are recorded the recording medium user identification data along with main data with recorder and player user identification data read from a data recorder and player"; claim 37, "encrypted data are recorded on the recording medium; and the main data read from the recording medium are decrypted using the recording medium user identification data as an encryption key when the recording medium user identification data are coincident with the recorder and player user identification data"; claim 41, "when the recording medium user identification data are coincident with the memory user identification data the controller allows the reproduction of the main data from the recording medium"; claim 42, "when the recording medium user identification data are coincident with the memory user identification data the controller decrypts the main data read by the head from the recording medium using the recording medium user identification"; claim 65, "comparing main data user identification data extracted from main data within which at least the main data user identification data are buried with read from a data recorder and player for reproduction of the main data; and reproducing the main data when the main data user identification data are coincident with the recorder and player user identification data"; claim 73, "the main data user identification data are decrypted using the main data user identification data when the main data user identification data are coincident with the recorder and player user identification data.

15. As per claim 34:

c. Regarding the limitations: "upon request, sending data stored in a storage unit provided in a server, said data having at least buried therein user identification information intended to identify a user and having been encrypted with the user identification information, to a recorder; causing the recorder to extract the user identification information from the received data; judging whether the extracted user identification information is coincident with user identification information held in an information holder provided in the recorder; and recording the received data to a recording medium when the extracted user identification information is coincident with the user identification information held in the information holder provided in the recorder,"

d. These limitations are recited in copending application no. 10,088,337, claim 33, "comparing recording medium user identification data read from a recording medium upon which are recorded the recording medium user identification data along with main data"; claim 37, "encrypted data are recorded on the recording medium; and the main data read from the recording medium are decrypted using the recording medium user identification data as an encryption key when the recording medium user identification data are coincident with the recorder and player user identification data"; claim 41, "when the recording medium user identification data are coincident with the memory user identification data the controller allows the reproduction of the main data from the recording medium"; claim 42, "when the recording medium user identification data are coincident with the memory user identification data the controller decrypts the main data read by the head from the recording medium using the recording medium user identification"; claim 65, "comparing main data user identification data extracted from main data within which at least the main data user identification data are buried with read from a data recorder and player for reproduction of the main data; and reproducing the main data when the main data user identification data are coincident with the recorder and player user identification data"; claim 73, "the main data user identification data are decrypted using the main data user identification data when the main data user identification data are coincident with the recorder and player user identification data.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Claim Rejections - 35 USC § 112

16. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

17. Claims 1-7 are rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential steps, such omission amounting to a gap between the steps. See MPEP § 2172.01. The omitted steps are:

e. when it is detected that the terminal unit is connected to the recorder, the recorder authenticates the terminal unit (Specification, pg. 22, last paragraph)- this step is essential since the exchanging of the encryption key only proceeds when the terminal unit is authenticated; without authentication, the exchanging step and encrypting step do not properly secure the recorded data; and

Claim Rejections - 35 USC § 102

18. Claim 34 is rejected under 35 USC 102(b) as being anticipated by Bjorn et al. PCT Publication No. WO9926373 (hereinafter Bjorn).

19. As per claim 34, Bjorn discloses a method of controlling data recording, wherein:

f. upon request, sending data stored in a storage unit provided in a server, said data having at least buried therein user identification information intended to identify a user and having been encrypted with the user identification information, to a recorder; causing a recorder to extract the user identification information from the received data; judging whether the extracted user identification information is coincident with user identification information held in an information holder provided in the recorder; and recording the received data to a recording medium when the extracted user identification information is coincident with the user identification information held in the information holder provided in the recorder (pg. 11-14; fig. 6).

20. Claim 16 is rejected under 35 U.S.C. 102(b) as being anticipated by Kupka PCT Publication Number WO0029928 (hereinafter Kupka).

21. As per claim 16, Kupka discloses a method of playing back a recording medium, comprising the steps of:

g. when a player is going to play back a recording medium containing user identification information, intended to identify a user, and data having been encrypted with the user identification information and stored in the recording medium therewith, judging whether user identification information read from an information holder provided in the player to hold user identification information sent from a terminal unit is coincident with user identification information read from the recording medium; and decrypting encrypted data read from the recording medium when the user identification information read from the information holder is coincident with that read from the recording medium (pg. 21, line 29-28, line 14, especially pg. 25, line 18-pg. 26, line 7).

Claim Rejections - 35 USC § 103

22. Claims 1-15 and 18 are rejected under 35 USC 103(a) as being unpatentable over Kupka, and further in view of Schneier Applied Cryptography, Chapter 2 (hereinafter Schneier).

23. As per claim 1, Kupka discloses a method for recording data to a recording medium, comprising steps of:

h. detecting, when a recorder is going to record data to the recording medium, whether a terminal unit with a memory having user identification information recorded therein is connected; (pg. 15, line 25-pg. 16, line 2; pg. 17, lines 13-22)

i. when it is detected that the terminal unit is connected, sending identification information from the terminal unit to the recorder; (pg. 17, line 23-pg. 20, line 13) and

j. encrypting the data to be recorded to the recording medium with the user identification information sent from the terminal unit and recording the encrypted data to the recording medium. (pg. 20, line 14-pg. 21, line 20)

24. Kupka does not disclose exchanging an encryption key between the player and the terminal unit, encrypting the user identification information with the exchanged encryption key, and sending the encrypted user identification information from the terminal unit to the player. Schneier discloses that the steps of transferring an encryption key for the purpose of encrypting the data with the transferred key and

securely transmitting the encrypted data are a conventional operation to secure transmitted data (Schneier, pgs. 31-32, "how Alice can send a message to Bob using public-key cryptography", steps 1-4). This procedure maintains the privacy of the data being transferred from unscrupulous 3rd parties. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to exchange an encryption key between the player and the terminal unit, encrypt the user identification information and transmit the encrypted identification information from the terminal unit to the player. One would be motivated to do so to keep the transmission private without requiring the terminal unit to store the encryption key value.

25. As per claims 2-4, the rejection of claim 1 under 35 USC 103(a) as being unpatentable over Kupka in view of Schneier is incorporated herein. (supra) In addition, Kupka discloses that the user identification information is provided by a terminal unit separate from the player but connected to the player. (the preferred embodiment discloses the terminal media as a ZIP disk) Furthermore, the step of detecting whether a terminal unit is connected to the card reader when received data is not properly identified is an obvious enhancement: any step that rechecks all the connection points for proper operation when a fault or error is identified is obvious because it facilitates the correct action to be taken by the user for proper operation. Further, the step of displaying an indication that the terminal unit is not connected when the terminal unit is not connected is an obvious enhancement since it identifies the problem to the user to facilitate corrective action to be taken for proper operation.

Moreover, the step of inhibiting output of data from the recording medium when the terminal unit is not successfully authenticated are obvious enhancements: any step that prevents access to information when a user does not have access is obvious because it ensures that only those with proper access has access to the data. Finally, the step of displaying an indication that a terminal unit has not been successfully authenticated is obvious since it facilitates the correct action to be taken by the user to be successfully authenticated. The aforementioned cover the limitations of claims 2-4.

26. As per claims 5-7, the rejection of claim 1 under 35 USC 103(a) is incorporated herein. (supra) Kupka does not disclose that the user sets the user information or that the user identification includes a username. However, the use of a username to identify a user is a standard operation in the computing arts. A username is typically an alphanumeric value that identifies one user or a group of users that correspond to an account by which the user or group of users have access to a service. Furthermore, to facilitate assigning a username relevant to the user, the username is ordinarily set by the user. For example, when a user registers an application, the user selects a name to identify the user/owner of the application. Examiner takes Official Notice of this teaching. It would be obvious to one of ordinary skill in the art at the time the invention was made for the user information to be set by the user and for the user identification to include a username. One would be motivated to do so to assign an identification value specific and relevant to the user so that the user identifies the username as their own. Finally, terminal unit identities are conventionally set at the time of shipment of the unit.

For example, MAC values are assigned by the producer of a terminal unit to uniquely identify the hardware from every other hardware. The aforementioned cover the limitations of claims 5-7.

27. As per claim 18, the rejection of claim 16 under 35 USC 102(b) is incorporated herein. (supra) Kupka does not disclose exchanging an encryption key between the player and the terminal unit, encrypting the user identification information with the exchanged encryption key, and sending the encrypted user identification information from the terminal unit to the player. Schneier discloses that the steps of transferring an encryption key for the purpose of encrypting the data with the transferred key and securely transmitting the encrypted data are a conventional operation to secure transmitted data (Schneier, pgs. 31-32, "how Alice can send a message to Bob using public-key cryptography", steps 1-4). This procedure maintains the privacy of the data being transferred from unscrupulous 3rd parties. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to exchange an encryption key between the player and the terminal unit, encrypt the user identification information and transmit the encrypted identification information from the terminal unit to the player. One would be motivated to do so to keep the transmission private without requiring the terminal unit to store the encryption key value.

28. As per claims 8-12, the rejection of claim 18 under 35 USC 103(a) is incorporated herein. (supra) In addition, Kupka discloses that the user identification

information is provided by a terminal unit separate from the player but connected to the player. (the preferred embodiment discloses the terminal media as a ZIP disk) Furthermore, the step of detecting whether a terminal unit is connected to the card reader when received data is not properly identified is an obvious enhancement: any step that rechecks all the connection points for proper operation when a fault or error is identified is obvious because it facilitates the correct action to be taken by the user for proper operation. Further, the step of displaying an indication that the terminal unit is not connected when the terminal unit is not connected is an obvious enhancement since it identifies the problem to the user to facilitate corrective action to be taken for proper operation. Moreover, the step of inhibiting output of data from the recording medium when the user identification information received from the terminal unit is not coincident with the user identification information read from the recording medium, or when the terminal unit is not successfully authenticated are obvious enhancements: any step that prevents access to information when a user does not have access is obvious because it ensures that only those with proper access has access to the data. Further, the step of displaying an indication that a terminal unit has not been successfully authenticated is obvious since it facilitates the correct action to be taken by the user to be successfully authenticated. The aforementioned cover the limitations of claims 8-12.

29. As per claims 13-15, the rejection of claim 8 under 35 USC 103(a) is incorporated herein. (supra) Kupka does not disclose that the user sets the user information or that the user identification includes a username. However, the use of a

username to identify a user is a standard operation in the computing arts. A username is typically an alphanumeric value that identifies one user or a group of users that correspond to an account by which the user or group of users have access to a service. Furthermore, to facilitate assigning a username relevant to the user, the username is ordinarily set by the user. For example, when a user registers an application, the user selects a name to identify the user/owner of the application. Examiner takes Official Notice of this teaching. It would be obvious to one of ordinary skill in the art at the time the invention was made for the user information to be set by the user and for the user identification to include a username. One would be motivated to do so to assign an identification value specific and relevant to the user so that the user identifies the username as their own. Finally, terminal unit identities are conventionally set at the time of shipment of the unit. For example, MAC values are assigned by the producer of a terminal unit to uniquely identify the hardware from every other hardware. The aforementioned cover the limitations of claims 13-15.

30. Claims 17 and 19-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kupka.

31. As per claims 17 and 19-22, the rejection of claim 16 under 35 USC 102(b) is incorporated herein. (supra) In addition, Kupka discloses that the user identification information is provided by a terminal unit separate from the player but connected to the player. (the preferred embodiment discloses the terminal media as a ZIP disk)

Furthermore, the step of detecting whether a terminal unit is connected to the card reader when received data is not properly identified is an obvious enhancement: any step that rechecks all the connection points for proper operation when a fault or error is identified is obvious because it facilitates the correct action to be taken by the user for proper operation. Further, the step of displaying an indication that the terminal unit is not connected when the terminal unit is not connected is an obvious enhancement since it identifies the problem to the user to facilitate corrective action to be taken for proper operation. Moreover, the step of inhibiting output of data from the recording medium when the user identification information received from the terminal unit is not coincident with the user identification information read from the recording medium, or when the terminal unit is not successfully authenticated are obvious enhancements: any step that prevents access to information when user does not have access is obvious because it ensures that only those with proper access has access to the data. Further, the step of displaying an indication that a terminal unit has not been successfully authenticated is obvious since it facilitates the correct action to be taken by the user to be successfully authenticated. The aforementioned cover the limitations of claims 17 and 19-22.

32. As per claims 23-25, the rejection of claims 17 and 20-22 under 35 USC 103(a) is incorporated herein. (supra) Kupka does not disclose that the user sets the user information or that the user identification includes a username. However, the use of a username to identify a user is a standard operation in the computing arts. A username is typically an alphanumeric value that identifies one user or a group of users that

correspond to an account by which the user or group of users have access to a service. Furthermore, to facilitate assigning a username relevant to the user, the username is ordinarily set by the user. For example, when a user registers an application, the user selects a name to identify the user/owner of the application. Examiner takes Official Notice of this teaching. It would be obvious to one of ordinary skill in the art at the time the invention was made for the user information to be set by the user and for the user identification to include a username. One would be motivated to do so to assign an identification value specific and relevant to the user so that the user identifies the username as their own. Finally, terminal unit identifies are conventionally set at the time of shipment of the unit. For example, MAC values are assigned by the producer of a terminal unit to uniquely identify the hardware from every other hardware. The aforementioned cover the limitations of claims 23-25.

33. Claim 35 is rejected under 35 USC 103(a) as being unpatentable over Bjorn and further in view of Ueno et al. USPN 4,999,661 (hereinafter Ueno).

34. As per claim 35, the rejection of claim 34 under 35 USC 102(b) as being anticipated by Bjorn is incorporated herein. (supra) Bjorn does not disclose the step of when it is judged that the user identification information extracted from the received data is not coincident with the user identification information held in the information holder in the player, it is judged whether user identification information in the received data is to be rewritten. However, the step of judging whether information is to be rewritten is a

typical operation to update values consistent with the current status or requirement of the apparatus. For example, Ueno discloses a device having multiple functions wherein the device judges whether certain data in memory needs to be rewritten based on the mode of the device (Ueno, col. 1:55-60; claim 11). It would be obvious to one of ordinary skill in the art at the time the invention was made to judge whether user identification information is to be rewritten when the extracted user identification information and the stored user identification information is not coincident. One would be motivated to do so to maintain values in memory consistent with the status of the device as known to one of ordinary skill in the art. The aforementioned cover the limitations of claim 35.

Allowable Subject Matter

35. Claims 26-33 and 47-58 are allowed

36. Claims 36-46 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W. Kim whose telephone number is (571) 272-3804. The examiner can normally be reached on M-F 9:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jung W Kim
Examiner
Art Unit 2132

June 1, 2006

Gilberto B

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100